Bash Bug (ShellShock)





October 2014

Background

A serious vulnerability exists in GNU Bash (Bourne again shell) processes and CVE-2014-6271 or CVE-2014-7169 exploitation may result in the ability for a remote attacker to override or bypass environment restrictions.

Bash is a Linux/Unix based command shell. The vulnerability found in versions 1.14.0 thru 4.3 allows an attacker to execute arbitrary code. The flaw in Bash includes the ability for additional text or trailing strings within a function definition or variable mistakenly being accepted as a command. This flaw bypasses restrictions that usually prohibit additional lines of text being accepted as commands. Vulnerable systems affected will receive and execute the delivered code. The exploitation may result in the ability for a remote attacker to override or bypass environment restrictions to execute shell commands before restrictions are applied.

Critical Internet-facing information systems providing services such as web and Domain Name System (DNS) are of the most concern as they may be vulnerable to immediate exploitation via the Bash vulnerability. The vulnerability also represents a threat to Industrial Control Systems/Supervisory Control and Data Acquisition (ICS/SCADA) systems as many run on Unix platforms that utilize Bash, are infrequently updated due to the need for high availability, or may have a vulnerable web interface.

Mitigation

There are multiple, well-written descriptions of the vulnerability which provide local tests for the vulnerability. These include the Redhat blog at https://securityblog.redhat.com/2014/09/24/bash-specially-crafted-environment-variables-code-injection-attack/and www.troyhunt.com/2014/09/everything-you-need-to-know-about.html.

Multiple vendors have already issued patches for the bug. As publicly-available official patches are released beyond software version 4.3, clients and servers should be upgraded to newer versions that are not affected by the vulnerability. Most OS X users are protected by default

settings because vulnerable services are turned off, but Apple has released patches for Lion, Mountain Lion, and Mavericks for users who have configured advanced Unix services.

For products that have not yet been patched, it is possible to manually patch by downloading and rebuilding Bash from the patched source code releases at ftp.gnu.org/gnu/bash/. The correct version will vary depending on the platform to be patched.

If unable to patch, system administrators should monitor affected systems for nefarious accesses and command-line activities at the device level, and disable unnecessary or unused services that can be used as an attack vector (e.g. CGI, SSH, SFTP). Additionally, there are various network-based mitigations (such as mod_security rules and IPTables rules) that may help to some extent until a patch can be implemented. More information on these network mitigations can be found at https://access.redhat.com/articles/1212303.

Beyond patching, administrators must also ensure that external input is validated before it is passed to backend processes. This is vital as the core issue with this vulnerability is content validation for externally provided input, similar to cross-site scripting (XSS) and SQL injection attacks. For detailed information on defending against input validation attacks, please see "Defending Against the Exploitation of SQL Vulnerabilities to Compromise a Network" at https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/fact_sheets.shtml

For further information, please contact your IAD Client Advocate. Military commands/services/agencies should call 410-854-4200, and Civil and Intelligence agencies should call 410-854-4790.

Disclaimer of Endorsement:

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government, and shall not be used for advertising or product endorsement purposes.

Bash Bug (ShellShock)



Contact Information

Industry Inquiries 410-854-6091 bao@nsa.gov

USG/IC Customer Inquiries 410-854-4790

DoD/Military/COCOM Customer Inquiries 410-854-4200

General Inquiries
NSA Information Assurance Service Center
niasc@nsa.gov